



Πολιτική Ασφάλειας Πληροφοριών

ΠΟ-00, 12.01.2026



Στοιχεία Εγγράφου

Τίτλος Εγγράφου	Πολιτική Ασφάλειας Πληροφοριών
Αρμόδιο Τμήμα	Διεύθυνση Πληροφορικής
Είδος Εγγράφου	Πολιτική Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
Κατηγορία	Δημόσια Χρήση
Κωδικός/ Έκδοση	ΠΟ-00
Ημερομηνία έκδοσης	12/01/2026

Πίνακας Ιστορικότητας Μεταβολών Εγγράφου

Έκδοση	Ημερομηνία	Περιγραφή μεταβολών
1.0	22/02/2025	Αρχική έκδοση



Περιεχόμενα

Στοιχεία Εγγράφου.....	2
Πίνακας Ιστορικότητας Μεταβολών Εγγράφου	2
Περιεχόμενα.....	3
1. Εισαγωγή	5
1.1 Γενικές Πληροφορίες	5
1.2 Θεσμικό και Εποπτικό Πλαίσιο.....	5
1.3 Πεδίο Εφαρμογής	5
1.4 Σκοπός και Δήλωση Στόχων.....	5
1.5 Αρμοδιότητες και Έλεγχος	6
1.6 Επισκόπηση, Αναθεώρηση και Τήρηση Αρχείου.....	7
1.7 Πρόγραμμα μη συμμόρφωσης.....	7
2. Ορισμοί	8
3. Οργάνωση Ασφάλειας Πληροφοριών	8
3.1 Εσωτερική Οργάνωση	8
4. Γενικές Αρχές Πολιτικής.....	9
4.1 Ελαχιστοποίηση Κινδύνων	9
4.2 Πρόσβαση Όπου Απαιτείται.....	9
4.3 Ακεραιότητα, Εμπιστευτικότητα και Διαθεσιμότητα.....	9
4.4 Προβλεπόμενη Χρήση Αγαθών	9
4.5 Περιστατικά Ασφαλείας	9
4.6 Περιστατικά Διαχείρισης Λειτουργικού Κινδύνου.....	10
4.7 Ενημέρωση Ασφάλειας Πληροφοριών	10
4.8 Μεταβολές Ρόλων και Αρμοδιοτήτων	10
4.9 Τρίτοι Πάροχοι και Εξωτερικοί Συνεργάτες.....	10
4.10 Πρακτικές Ασφαλείας	11
4.11 Ιδιοκτήτες Πληροφοριών.....	11
5. Ασφάλεια Ανθρώπινου Δυναμικού	11
5.1 Πριν από την Απασχόληση	11
5.2 Κατά τη Διάρκεια της Απασχόλησης.....	12
5.3 Λήξη ή Μεταβολή Απασχόλησης	12



6.	Διαχείριση Αγαθών	13
7.	Διαβάθμιση Πληροφοριών	13
8.	Έλεγχος Πρόσβασης	13
8.1	Επιχειρησιακή Απαιτήση για τον Έλεγχο της Πρόσβασης	14
8.2	Ευθύνες Χρηστών	14
8.3	Έλεγχος Πρόσβασης σε Λειτουργικά Συστήματα και Εφαρμογές	14
8.4	Φορητά Μέσα Ηλεκτρονικών Υπολογιστών	14
8.5	Φορητές Ιδιωτικές Συσκευές (BYOD)	15
9.	Τηλεργασία	15
9.1	Εξοπλισμός	16
9.2	Επικοινωνίες	17
9.3	Λήψη αντιγράφων ασφαλείας στην Τηλεργασία	17
9.4	Καταγγελία Σύμβασης	17
10.	Πολιτική Κρυπτογραφίας	17
11.	Φυσική και Περιβαλλοντική Ασφάλεια	18
11.1	Ασφαλείς Περιοχές	18
11.2	Ασφάλεια Εξοπλισμού	19
12.	Ασφάλεια Επιχειρησιακών Λειτουργιών	19
12.1	Λειτουργικές Διαδικασίες	19
13.	Ασφάλεια Δικτύων και Επικοινωνιών	20
14.	Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων	20
15.	Διαχείριση Περιστατικών Ασφάλειας	21
16.	Διαχείριση Επιχειρησιακής Συνέχειας	21
17.	Λίστα Πολιτικών, Διαδικασιών & Φορμών	21
17.1	Πίνακας Πολιτικών	Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.
17.2	Πίνακας Διαδικασιών	Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.
17.3	Φόρμες και Σχέδια	Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.





1. Εισαγωγή

1.1 Γενικές Πληροφορίες

Η Πολιτική Ασφάλειας Πληροφοριών («Γενική Πολιτική Ασφάλειας» / «Πολιτική») αποτελεί μέρος του Κανονισμού Λειτουργίας και Εταιρικής Διακυβέρνησης της RENER ENERGY A.E. (εφεξής η «Εταιρεία»), έχει εγκριθεί από την Διοίκηση και τίθεται σε ισχύ από 22.07.2026.

1.2 Θεσμικό και Εποπτικό Πλαίσιο

Η Πολιτική συμμορφώνεται κατά κύριο λόγο, με την ακόλουθη νομοθεσία:

Γενικός Κανονισμός Προστασίας Δεδομένων, του ν. 4624/2019, του ν. 3471/2006 και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Για την αποτελεσματική διαχείριση της πιθανότητας έκθεσης σε κίνδυνο και της επικινδυνότητας, η παρούσα πολιτική καλύπτει τις θεματικές ενότητες ασφάλειας πληροφοριών όπως αυτές αναφέρονται αλλά και εναρμονίζονται και με το διεθνές πρότυπο ISO 27001:2022.

1.3 Πεδίο Εφαρμογής

Η Πολιτική υιοθετείται και εφαρμόζεται από:

- Τα πρόσωπα που διοικούν την Εταιρεία.
- Το σύνολο του προσωπικού της Εταιρείας, καθώς και όλους τους δημόσιους και ιδιωτικούς φορείς, εταιρείες και οργανισμούς με τους συνεργάζεται ή συναλλάσσεται η Εταιρεία.

1.4 Σκοπός και Δήλωση Στόχων

Σκοπός της παρούσας Πολιτικής είναι η διασφάλιση της **εμπιστευτικότητας**, της **ακεραιότητας** και της **διαθεσιμότητας** των πληροφοριών και συστημάτων της Εταιρείας, σύμφωνα με την κρισιμότητά τους για την επίτευξη των επιχειρησιακών στόχων, καθώς και της συμμόρφωσής του με το ισχύον νομοθετικό και ρυθμιστικό πλαίσιο.



Η Πολιτική Ασφάλειας αποτελεί το σύνολο, των κανόνων, των διαδικασιών, των ρόλων και των αρμοδιοτήτων για τη διασφάλιση της προστασίας των πληροφοριακών συστημάτων της Εταιρείας και την εύρυθμη επιχειρησιακή του συνέχεια.

Βάσει της Πολιτικής Ασφάλειας Πληροφοριών η Εταιρεία θεσπίζει Πολιτικές Διαχείρισης της Ασφάλειας Πληροφοριών και εφαρμόζει πιο συγκεκριμένες διαδικασίες ασφάλειας πληροφοριών καθώς και μέτρα ασφάλειας, μεταξύ άλλων για τη μείωση των κινδύνων που μπορεί να εκτεθεί. Στην παρούσα πολιτική περιγράφονται οι βασικές αρχές για τις οποίες καταγράφονται οι εν λόγω διαδικασίες.

1.5 Αρμοδιότητες και Έλεγχος

1. Διοίκηση
2. Υπεύθυνος Πληροφορικής / CISO (ή Υπεύθυνος Πληροφορικής)
3. Εξωτερικός Ελεγκτής / Σύμβουλος: υποστηρικτικός ή/και ανεξάρτητος ελεγκτικός ρόλος

Κατηγορία	Ενέργεια	Διοίκηση	Υπεύθυνος Πληροφορικής / CISO / IT	Εξωτερικός Ελεγκτής / Σύμβουλος
Πολιτική	Παροχή κατευθυντήριων γραμμών, βασικών αρχών και στόχων διακυβέρνησης	✓		
	Ανάπτυξη / Επικαιροποίηση Πολιτικής		✓	Υποστήριξη (όπου απαιτείται)
	Έγκριση Πολιτικής	✓		
	Υπεύθυνος Πολιτικής		✓	
	Επισκόπηση Πολιτικής		✓	
	Γνωστοποίηση Πολιτικής	✓	✓	
	Διασφάλιση επισκόπησης και επικαιροποίησης Πολιτικής	✓		
	Εποπτεία εφαρμογής Πολιτικής	✓		



Εφαρμογή, επισκόπηση και έλεγχος	Παραγωγή Αναφορών		✓	Υποστήριξη (όπου απαιτείται)
	Διενέργεια ελέγχου εφαρμογής της εγκεκριμένης Πολιτικής / Επισκόπηση αναφορών	✓		✓ (όπου απαιτείται)

Αναφορικά με τη διασφάλιση, την προστασία και την ενημέρωση σε θέματα δεδομένων προσωπικού χαρακτήρα, αρμόδιος είναι ο Υπεύθυνος Προστασίας Δεδομένων (DPO) όπως έχει οριστεί από την Εταιρεία. Η Διοίκηση της Εταιρείας διασφαλίζει πως το σύστημα διακυβέρνησης της Εταιρείας και ιδίως το σύστημα ΣΔΑΠ διαχειρίζεται επαρκώς τους κινδύνους ΤΠΕ και ασφάλειας της Εταιρείας.

Η Διοίκηση της Εταιρείας διασφαλίζει την επάρκεια του προσωπικού, τόσο σε πληρότητα όσο και ως προς τις δεξιότητες που αυτό διαθέτει.

1.6 Επισκόπηση, Αναθεώρηση και Τήρηση Αρχείου

Η παρούσα Πολιτική επισκοπείται ετησίως από τον Υπεύθυνο Πληροφορικής / CISO. Αναθεώρηση της Πολιτικής ενδέχεται να πραγματοποιηθεί εκτάκτως όποτε το απαιτούν οι περιστάσεις λόγω μεταβολών είτε στο νομο-κανονιστικό πλαίσιο είτε σε συναφείς πολιτικές και διαδικασίες, έτσι ώστε να ανταποκρίνεται στις εκάστοτε ισχύουσες συνθήκες.

Ο Υπεύθυνος Πληροφορικής / CISO είναι υπεύθυνος για τη διατήρηση σε ηλεκτρονική μορφή των εκδόσεων της Πολιτικής, καθώς και για τη διατήρηση φύλλου παρακολούθησης των τροποποιήσεων της, έτσι ώστε να είναι άμεσα διαθέσιμη και προσβάσιμη στα πρόσωπα που εμπίπτουν σε αυτήν. Επίσης είναι υπεύθυνος να γνωστοποιεί στα εμπλεκόμενα μέρη την Πολιτική καθώς και τυχόν τροποποιήσεις αυτής δια της κοινοποιήσεως της μέσω οποιουδήποτε πρόσφορου μέσου, αρκεί να δύναται να αποδεικνύεται η ενημέρωση αυτών.

1.7 Πρόγραμμα μη συμμόρφωσης

Σε περίπτωση που οποιοσδήποτε εργαζόμενος της Εταιρείας αντιληφθεί πραγματική ή δυνητική μη συμμόρφωση με την παρούσα Πολιτική που θα έχει ως αποτέλεσμα την παραβίαση της εμπιστευτικότητας, της ακεραιότητας ή / και της διαθεσιμότητας των πληροφοριακών συστημάτων και πληροφοριών της Εταιρείας μη εφαρμογή της Πολιτικής ενημερώνει άμεσα τον Υπεύθυνο Πληροφορικής / CISO ή σε περίπτωση απουσίας του τον Νόμιμο Εκπρόσωπο της Εταιρείας. Η αρμόδια λειτουργία αξιολογεί την αναφορά και λαμβάνει τα αναγκαία διορθωτικά



ή/και προληπτικά μέτρα ή, εφόσον απαιτείται, εισηγείται το θέμα στον Νόμιμο Εκπρόσωπο, ο οποίος αποφασίζει για την επιβολή τυχόν πειθαρχικών κυρώσεων.

2. Ορισμοί

Πολιτική: Η Πολιτική Ασφάλειας Πληροφοριών

ΤΠΕ: Τεχνολογίες Πληροφοριών και Επικοινωνίας

Πληροφοριακό Σύστημα: Είναι ένα οργανωμένο σύνολο που αποτελείται από πέντε στοιχεία: Ανθρώπους, υλικό, λογισμικό, διαδικασίες και δεδομένα, τα οποία αλληλοεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση πληροφορίας για την υποστήριξη ανθρώπινων δραστηριοτήτων, στο πλαίσιο ενός οργανισμού.

Ακεραιότητα: Η διασφάλιση της ακρίβειας και της πληρότητας της πληροφορίας.

Διαθεσιμότητα: Η διασφάλιση της διαθεσιμότητας της πληροφορίας και των πληροφοριακών πόρων στη διάθεση των χρηστών όποτε αυτό απαιτείται.

Εμπιστευτικότητα: Η διασφάλιση ότι πληροφορίες δε θα αποκαλύπτονται (δημοσιοποιούνται) σε μη εξουσιοδοτημένα πρόσωπα, φορείς, διαδικασίες ή συστήματα.

3. Οργάνωση Ασφάλειας Πληροφοριών

3.1 Εσωτερική Οργάνωση

Η Εταιρεία τηρεί ένα πλαίσιο ασφάλειας πληροφοριακών συστημάτων και πληροφοριών προκειμένου να διαχειρίζεται αποτελεσματικότερα την ασφάλειά τους. Το πλαίσιο ασφάλειας εναρμονίζεται πλήρως, τόσο με την φύση των πληροφοριακών αγαθών και των επιχειρησιακών απαιτήσεων της Εταιρείας, όσο και με την πολυπλοκότητα των δραστηριοτήτων που καλείται να διαχειριστεί η Εταιρεία.

Η Εταιρεία διατηρεί κατάλληλο διοικητικό σχήμα το οποίο:

- Εξασφαλίζει ότι η Εταιρεία διαθέτει τους απαραίτητους πόρους για την αποτελεσματική εφαρμογή της Πολιτικής.
- Αναθέτει τους ρόλους και τις αρμοδιότητες σε σχέση με την ασφάλεια πληροφοριών.
- Συντονίζει την υλοποίηση του προγράμματος της ασφάλειας πληροφοριών στην Εταιρεία.
- Διασφαλίζει ότι οι στόχοι της Πολιτικής είναι ευθυγραμμισμένοι με τους γενικότερους στόχους της Εταιρείας.
- Η καθιέρωση και η επιτυχής εφαρμογή της Πολιτικής απαιτούν τη συνεργασία όλων όσων εμπλέκονται στην επίτευξη των επιχειρησιακών στόχων της Εταιρείας: Της Διοίκησης, των στελεχών, των χρηστών, των προμηθευτών, των αναδόχων, των επισκεπτών και των τρίτων συνεργαζόμενων φορέων.



- Η Εταιρεία θα τηρεί σαφώς καθορισμένους ρόλους και αρμοδιότητες για το σύνολο των στελεχών, υπαλλήλων, συνεργατών και τρίτων μερών, σύμφωνα με την «Πολιτική Οργάνωσης Ασφάλειας Πληροφοριακών Συστημάτων & Πληροφοριών».

4. Γενικές Αρχές Πολιτικής

4.1 Ελαχιστοποίηση Κινδύνων

Η ασφάλεια των πληροφοριών και πληροφοριακών συστημάτων της Εταιρείας αποτελεί στρατηγικής σημασίας στόχο και υποχρέωσή της. Η Εταιρεία εφαρμόζει μια πολιτική μέσω της οποίας είναι σε θέση να επιβλέπει και να ελέγχει την ασφάλεια των πληροφοριακών του αγαθών ώστε να είναι σε θέση να ελαχιστοποιεί τους κινδύνους και τις πιθανές επιπτώσεις τους.

4.2 Πρόσβαση Όπου Απαιτείται

Τα πληροφοριακά συστήματα της Εταιρείας, καθώς και οι πληροφορίες σε φυσική / έντυπη μορφή, αποτελούν απαραίτητους πόρους για την επίτευξη των επιχειρησιακών της στόχων. Η Εταιρεία παρέχει πρόσβαση στις πληροφορίες του μόνο στα άτομα που απαιτούνται για την επίτευξη των επιχειρησιακών του στόχων («need to know» principle).

4.3 Ακεραιότητα, Εμπιστευτικότητα και Διαθεσιμότητα

Τα πληροφοριακά συστήματα, καθώς και οι πληροφορίες της Εταιρείας διαχειρίζονται και να χρησιμοποιούνται κατάλληλα, ώστε να διασφαλίζεται η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητά τους.

4.4 Προβλεπόμενη Χρήση Αγαθών

Τα πληροφοριακά συστήματα και οι πληροφορίες αποτελούν αγαθό της Εταιρείας και μπορούν να χρησιμοποιηθούν μόνο για την επίτευξη των επιχειρησιακών στόχων της. Η χρήση τους από το προσωπικό της Εταιρείας ή τρίτους με σκοπό την αποκόμιση προσωπικού κέρδους, τη διεξαγωγή επιχειρηματικών δραστηριοτήτων εκτός αυτών της Εταιρείας ή με σκοπό να διαπράξουν αξιόποινες πράξεις δεν επιτρέπεται. Για περισσότερες πληροφορίες δείτε «Πολιτική Αποδεκτής Διαχείρισης Αγαθών».

4.5 Περιστατικά Ασφαλείας

Πληροφορίες μη κατηγοριοποιημένες ως «Δημόσιες» πρέπει να προστατεύονται και δεν πρέπει να δημοσιοποιούνται χωρίς την κατάλληλη έγκριση. Μη εξουσιοδοτημένη πρόσβαση, διαχείριση,





δημοσιοποίηση ή αναπαραγωγή και μετάδοση αυτών των πληροφοριών διακυβεύει την ασφάλεια της Εταιρείας, αποτελεί «Περιστατικό Ασφάλειας».

4.6 Περιστατικά Διαχείρισης Λειτουργικού Κινδύνου

Η ασφάλεια πληροφοριών αποτελεί ένα ζήτημα διαχείρισης λειτουργικού κινδύνου. Σε όλες τις Διευθύνσεις και τα Τμήματα της Εταιρείας εφαρμόζονται βέλτιστες πρακτικές (σύμφωνα με τη «Πολιτική Αποδεκτής Διαχείρισης Αγαθών») και δικλείδες ασφάλειας προς ελαχιστοποίηση των κινδύνων.

4.7 Ενημέρωση Ασφάλειας Πληροφοριών

Περιστατικά ασφάλειας πρέπει να αναφέρονται άμεσα αρχικά στον Υπεύθυνο Πληροφορικής / CISO, ο οποίος είναι αρμόδιος να αξιολογήσει τη σοβαρότητα και να λάβει τα κατάλληλα μέτρα και εν συνεχεία στο Τμήμα Πληροφορικής.

4.8 Μεταβολές Ρόλων και Αρμοδιοτήτων

Όλες τα Τμήματα της Εταιρείας παρέχουν άμεση ενημέρωση στους διαχειριστές συστημάτων και στο Υπεύθυνο / CISO αναφορικά με μεταβολές στην εργασιακή θέση, το ρόλο και τις αρμοδιότητες μέσα στην Εταιρεία (μεταθέσεις, αποχωρήσεις, προσλήψεις, έναρξη συνεργασίας κ.λπ.) των υπάλληλων, συνεργατών ή τρίτων, οι οποίες χρήζουν απόδοσης ή μεταβολής δικαιωμάτων πρόσβασης στα πληροφοριακά συστήματα της Εταιρείας.

4.9 Τρίτοι Πάροχοι και Εξωτερικοί Συνεργάτες

Όλοι οι τρίτοι πάροχοι υπηρεσιών ή εξωτερικοί συνεργάτες που επεξεργάζονται, αποθηκεύουν ή έχουν πρόσβαση σε πληροφοριακά συστήματα ή δεδομένα της Εταιρείας υπόκεινται σε διαδικασίες αξιολόγησης, έγκρισης και συνεχούς παρακολούθησης από τα αρμόδια Τμήματα και το τμήμα Ασφάλειας Πληροφοριών ή Μηχανογράφησης. Πριν από την έναρξη οποιασδήποτε συνεργασίας, τεκμηριώνονται και συμφωνούνται σαφείς τεχνικές και οργανωτικές απαιτήσεις, συμπεριλαμβανομένων εκείνων που απορρέουν από το ισχύον κανονιστικό πλαίσιο και ιδίως από το πρότυπο ISO 27001 σχετικά με τη ΣΔΑΠ. Η Εταιρεία διασφαλίζει ότι κάθε πάροχος εφαρμόζει κατάλληλα μέτρα ασφάλειας, συμμορφώνεται με τις συμβατικές υποχρεώσεις και παρέχει έγκαιρη ενημέρωση για κάθε αλλαγή υπηρεσίας, περιστατικό ασφάλειας ή άλλο γεγονός που δύναται να επηρεάσει τη διαθεσιμότητα, την ακεραιότητα ή την εμπιστευτικότητα των πληροφοριών της Εταιρείας.





4.10 Πρακτικές Ασφαλείας

Ο Υπεύθυνος Πληροφορικής / CISO και το τμήμα Ασφάλειας Πληροφοριών ή Πληροφορικής είναι αρμόδιοι να δημιουργούν και να προάγουν κατάλληλες πρακτικές ασφαλείας (security practices) στο σύνολο της Εταιρείας, συμπεριλαμβανομένων:

- Ενημερώσεων σε υφιστάμενο και νέο προσωπικό.
- Προγραμμάτων ενίσχυσης της κουλτούρας κινδύνων / ευαισθητοποίησης Ασφάλειας Πληροφοριών (Information Security Awareness).

4.11 Ιδιοκτήτες Πληροφοριών

Η Εταιρεία προσδιορίζει εγγράφως όλους τους «ιδιοκτήτες πληροφοριών» για το σύνολο των Πληροφοριακών συστημάτων και κατηγοριών πληροφοριών.

5. Ασφάλεια Ανθρώπινου Δυναμικού

Η Εταιρεία εξασφαλίζει ότι όλοι οι χρήστες (υπάλληλοι, ανάδοχοι, τρίτοι) κατανοούν τις ευθύνες τους σχετικά με την ασφάλεια πληροφοριών και ότι είναι κατάλληλοι για τους ρόλους για τους οποίους έχουν επιλεγεί. Η πολιτική ασφαλείας ανθρώπινου δυναμικού έχει ως σκοπό την ελαχιστοποίηση των κινδύνων από ανθρώπινο λάθος, κλοπή και σκόπιμο ή ακούσιο κακό χειρισμό των πληροφοριακών αγαθών της Εταιρείας, καθώς επίσης την ενσωμάτωση της ασφαλείας πληροφοριών στις περιγραφές εργασίας και τις διαδικασίες πρόσληψης προσωπικού.

5.1 Πριν από την Απασχόληση

Η Εταιρεία λαμβάνει μέριμνα ώστε να ελαχιστοποιείται η πιθανότητα πρόσληψης προσωπικού που μπορεί να τον θέσει σε κίνδυνο, όπου αυτό είναι εφικτό και σύμφωνα με το υφιστάμενο νομικό και κανονιστικό πλαίσιο. Ιδιαίτερη μέριμνα θα λαμβάνεται για προσλήψεις που αφορούν καίριες θέσεις της Εταιρείας, συμπεριλαμβανομένων αυτών που σχετίζονται με την επεξεργασία ευαίσθητων δεδομένων.

Πολιτική Επιλογής Προσωπικού (Personnel Screening Policy)

Η Εταιρεία θα διεξάγει ελέγχους επαλήθευσης των στοιχείων όλων των υποψηφίων και ειδικότερα σε επιλογή προσωπικού σε θέσεις οι οποίες έχουν σαν προϋπόθεση αυξημένες απαιτήσεις ασφαλείας, σύμφωνα με τους σχετικούς νόμους και κανονισμούς, εφόσον αυτό κρίνεται απαραίτητο. Για τη διασφάλιση της ακεραιότητας και εμπιστευτικότητας των εταιρικών δεδομένων, το προσωπικό της Εταιρείας που θα εμπλέκεται σε επεξεργασία προσωπικών δεδομένων και ευαίσθητων εταιρικών πληροφοριών, θα πρέπει να διαθέτει επάρκεια γνώσεων και κατάρτιση στο χειρισμό αντίστοιχου τύπου δεδομένων. Τα δεδομένα των υποψηφίων υπαλλήλων που



συλλέγονται θα πρέπει να περιορίζονται στα απολύτως αναγκαία. Τα παραπάνω ισχύουν επίσης για έκτακτο προσωπικό καθώς και για τους εξωτερικούς συνεργάτες της Εταιρείας. Ιδιαίτερα για προσωπικό το οποίο επιλέγεται με τη βοήθεια κάποιου γραφείου ευρέσεως στελεχών ή ανήκει σε τρίτες εταιρίες (outsourced), οι ευθύνες τους έναντι της Εταιρείας θα πρέπει να είναι ξεκάθαρες.

Όροι και Συνθήκες Απασχόλησης

Η Εταιρεία μέσω του Τμήματος Ανθρώπινου Δυναμικού, μεριμνά ώστε κάθε νέος εργαζόμενος να ενημερώνεται για τις ευθύνες και τις αρμοδιότητές του σχετικά με την ασφάλεια πληροφοριών, οι οποίες θα προβλέπονται και από τη σύμβαση εργασίας. Ειδικότερα εξωτερικοί συνεργάτες οι οποίοι απασχολούνται σε θέσεις που τους παρέχουν πρόσβαση σε διαβαθμισμένες πληροφορίες, θα υπογράφουν σχετική συμφωνία εμπιστευτικότητας και μη δημοσιοποίησης πληροφοριών κατά την ανάληψη των καθηκόντων τους. Οι συμφωνίες εμπιστευτικότητας θα εξετάζονται και θα αναθεωρούνται όταν υπάρχουν μεταβολές σε συμβάσεις ή συμβόλαια με υπαλλήλους ή τρίτα μέρη.

5.2 Κατά τη Διάρκεια της Απασχόλησης

Όλοι όσοι εργάζονται στην Εταιρεία θα εφαρμόζουν τις πολιτικές και τις διαδικασίες ασφάλειας και θα τους γίνονται περιοδικές υπενθυμίσεις σχετικά με τις υποχρεώσεις που απορρέουν από την Πολιτική. Η Διοίκηση εξασφαλίζει ότι το σύνολο του προσωπικού της Εταιρείας, καθώς και τρίτα μέρη κατά περίπτωση, θα λαμβάνουν κατάλληλη ενημέρωση για την Πολιτική Ασφαλείας και τις σχετικές με αυτή διαδικασίες. Στο πλαίσιο αυτό θα εφαρμόζεται ένα περιοδικό πρόγραμμα αύξησης της επίγνωσης κινδύνων (awareness campaign) του προσωπικού του προσαρμοσμένο στις ανάγκες της Εταιρείας.

Σε όλο το νέο προσωπικό της Εταιρείας υποχρεωτικά θα γίνεται τεκμηριωμένη ενημέρωση / εκπαίδευση σε θέματα ασφάλειας πληροφοριών κατά την περίοδο της ένταξης / προσαρμογής τους στο εργασιακό περιβάλλον της Εταιρείας, πριν αποκτήσουν πρόσβαση σε προσωπικά και ευαίσθητα δεδομένα, απόρρητες πληροφορίες ή πληροφοριακά συστήματα.

5.3 Λήξη ή Μεταβολή Απασχόλησης

Σε περίπτωση μεταβολής της θέσης κάποιου εργαζομένου, οι ανάγκες του σε θέματα ασφάλειας πληροφοριών θα επαναξιολογούνται και εάν κρίνεται απαραίτητο, θα του παρέχεται η ανάλογη ενημέρωση.

Κατά τη διαδικασία λήξης της εργασιακής σχέσης με την Εταιρεία, όλοι οι χρήστες (υπάλληλοι, ανάδοχοι, τρίτοι) των πληροφοριακών συστημάτων θα επιστρέφουν τον εξοπλισμό (φορητοί υπολογιστές, κινητά τηλέφωνα, κ.λπ.) που τους παρασχέθηκε για την εκπλήρωση των εργασιών τους, όπως περιγράφεται στη «Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας». Επιπλέον θα επιστρέφεται στην Εταιρεία οποιοσδήποτε άλλος πληροφοριακός πόρος τους έχει παρασχεθεί,





όπως για παράδειγμα εγχειρίδια και πληροφορίες που βρίσκονται αποθηκευμένες σε ηλεκτρονικά μέσα κλπ.

Σε περιπτώσεις που υπάλληλοι, ανάδοχοι, τρίτοι, χρησιμοποιούν δικό τους εξοπλισμό, θα πρέπει να διασφαλίζεται ότι τυχόν ευαίσθητες πληροφορίες της Εταιρείας που είναι αποθηκευμένες στον εν λόγω εξοπλισμό θα διαγράφονται.

Τα δικαιώματα πρόσβασης του προσωπικού στα πληροφοριακά συστήματα της Εταιρείας, όπως και τα δικαιώματα φυσικής πρόσβαση στις εγκαταστάσεις της Εταιρείας θα αλλάζουν ή θα καταργούνται με μέριμνα του Υπεύθυνου Πληροφορικής, όταν η εργασιακή σχέση του ατόμου αυτού παύει ή μεταβάλλεται αντίστοιχα. Στις περιπτώσεις λήξης της εργασιακής σχέσης, οι εργαζόμενοι θα επιστρέφουν στον Συνεταιρισμό τις ειδικές κάρτες που τους είχαν δοθεί για την πρόσβαση στα γραφεία της Εταιρείας, όπως περιγράφεται στη «Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας».

Συμφωνίες εμπιστευτικότητας και μη δημοσιοποίησης ευαίσθητων πληροφοριών που εξακολουθούν να ισχύουν μετά την λήξη της απασχόλησης θα καθορίζονται, θα επικοινωνούνται στον υπάλληλο και θα πρέπει να εφαρμόζονται.

6. Διαχείριση Αγαθών

Στην «Πολιτική Αποδεκτής Διαχείρισης Αγαθών» προβλέπεται πως η Εταιρεία, για κάθε ένα από τα πληροφοριακά αγαθά της, προσδιορίζει «ιδιοκτήτες» και αναπτύσσει τα κατάλληλα μέτρα για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, τροποποίησης και καταστροφής τους, αποσκοπώντας στη διατήρηση ενός κατάλληλου επιπέδου προστασίας τους.

7. Διαβάθμιση Πληροφοριών

Σύμφωνα με την «Πολιτική Διαβάθμισης Πληροφοριών», οι πληροφορίες της Εταιρείας διαβαθμίζονται με κριτήριο το βαθμό ευαισθησίας τους, τις συνέπειες από πιθανή απώλειά τους ή από πιθανή απώλεια της εμπιστευτικότητάς τους, καθώς και σύμφωνα με τις υποχρεώσεις που η Εταιρεία φέρει απέναντι στη νομοθεσία στην οποία υπόκειται.

8. Έλεγχος Πρόσβασης

Η πρόσβαση στα Πληροφοριακά Συστήματα της Εταιρείας είναι περιορισμένη και ελεγχόμενη σύμφωνα με την «Πολιτική Ελέγχου Πρόσβασης», έτσι ώστε να διασφαλίζεται πως μόνο εξουσιοδοτημένοι και τακτοποιημένοι χρήστες έχουν δικαιώματα πρόσβασης στους πόρους και τις πληροφορίες της Εταιρείας.





8.1 Επιχειρησιακή Απαιτήση για τον Έλεγχο της Πρόσβασης

Πριν από την παραχώρηση πρόσβασης σε οποιοδήποτε πληροφοριακό πόρο εξετάζεται η επιχειρησιακή αναγκαιότητα ώστε να διασφαλίζεται η ασφάλεια των πληροφοριών της Εταιρείας. Εφαρμόζεται πολιτική ελέγχου πρόσβασης, σύμφωνα με τις επιχειρησιακές απαιτήσεις της Εταιρείας.

Η πρόσβαση στα πληροφοριακά συστήματα πρέπει να διασφαλίζεται από μέτρα ταυτοποίησης του χρήστη και καθορισμού του επιπέδου πρόσβασής του. Η πρόσβαση στα πληροφοριακά συστήματα πρέπει να είναι επαρκής αλλά ποτέ μεγαλύτερη των απαιτήσεων των χρηστών για την εκπλήρωση του επιχειρησιακού τους ρόλου και έργου.

Διαχείριση Πρόσβασης Χρηστών

Όλα τα τμήματα πρέπει να εφαρμόζουν τυποποιημένη διαδικασία, με την οποία καταγράφονται οι απαιτούμενες μεταβολές και αναφέρονται στον Υπεύθυνο Πληροφορικής / CISO, ώστε τα δικαιώματα των χρηστών να μεταβάλλονται ή να καταργούνται άμεσα. Η απόδοση των δικαιωμάτων πρέπει να βασίζεται στην αρχή των ελάχιστων προνομίων.

8.2 Ευθύνες Χρηστών

Όλοι οι χρήστες των πληροφοριακών συστημάτων πρέπει να ακολουθούν πρακτικές ασφάλειας καθορισμένες από την Εταιρεία που αφορούν στην επιλογή και στη χρήση των κωδικών πρόσβασης. Όλοι οι χρήστες της Εταιρείας λαμβάνουν τα απαραίτητα μέτρα για την προστασία των πληροφοριών και του πληροφοριακού εξοπλισμού που βρίσκονται στον χώρο εργασίας τους.

8.3 Έλεγχος Πρόσβασης σε Λειτουργικά Συστήματα και Εφαρμογές

Σε όλους τους χρήστες παρέχεται ένα μοναδικής ταυτότητας αναγνωριστικό χρήστη (user ID) για προσωπική τους χρήση, ενώ η πρόσβαση στα λειτουργικά συστήματα ελέγχεται μέσω μιας ασφαλούς διαδικασίας σύνδεσης, η οποία περιλαμβάνει κατ' ελάχιστον τη χρήση ισχυρού κωδικού πρόσβασης.

Οι κωδικοί πρόσβασης είναι αυστηρώς προσωπικοί και δεν κοινοποιούνται ή αποκαλύπτονται. Για την καλύτερη προστασία των κρίσιμων εφαρμογών, οι ανενεργές συνδέσεις διακόπτονται μετά από μια καθορισμένη περίοδο αδράνειας.

8.4 Φορητά Μέσα Ηλεκτρονικών Υπολογιστών

Η χρήση φορητών ηλεκτρονικών υπολογιστών απαιτεί έγκριση από τον Υπεύθυνο Πληροφορικής / CISO. Η χρήση αποσπώμενων αποθηκευτικών μέσων (USB Flash drives, External Disks κ.λπ.)





περιορίζεται μέσω σχετικού μηχανισμού και επιτρέπεται όπου απαιτείται για την εκπλήρωση των επιχειρησιακών αναγκών.

8.5 Φορητές Ιδιωτικές Συσκευές (BYOD)

Ως φορητές, ιδιωτικές συσκευές θεωρούνται, μεταξύ άλλων, οι εξής:

- Συσκευές Tablet.
- Έξυπνα κινητά.
- Φορητοί υπολογιστές.
- Έξυπνες συσκευές (wearables π.χ. έξυπνα ρολόγια, έξυπνα γυαλιά, κλπ.)

Η παραχώρηση άδειας στον εργαζόμενο, ώστε να κάνει χρήση δικών του συσκευών για επαγγελματικούς σκοπούς μπορεί να οδηγήσει στην ανάγκη υλοποίησης πρόσθετων ελέγχων και μέτρων προστασίας στις συσκευές αυτές, πέραν εκείνων που λαμβάνονται για μια απλή συσκευή προσωπικής χρήσης.

Συνηθισμένα προβλήματα σε σχέση με τη χρήση φορητών, ιδιωτικών συσκευών περιλαμβάνουν:

- Χρήση της συσκευής από άλλα μέλη της οικογένειας του υπαλλήλου.
- Προεπιλεγμένη αποθήκευση των δεδομένων σε εγκαταστάσεις υπολογιστικού νέφους (Cloud).
- Αυξημένη έκθεση σε κίνδυνο πιθανής απώλειας (πχ. χρήστη σε καφετέρια κλπ.)
- Πρόσβαση σε δικτυακούς τόπους που δεν πληρούν την Πολιτική Αποδεκτή Χρήσης Διαδικτύου της Εταιρείας.
- Σύνδεση σε μη ασφαλή δίκτυα.
- Έλλειψη προστασίας από ιούς και έλλειψη ενημέρωσης αντιικού λογισμικού.
- Εγκατάσταση δυνητικά κακόβουλων εφαρμογών στη συσκευή (συχνά χωρίς να γνωρίζει ο χρήστης ότι είναι κακόβουλες).

Τα θέματα αυτά λαμβάνονται υπόψη κατά την αξιολόγηση της καταλληλότητας οποιασδήποτε τέτοιας συσκευής, πριν καταστεί ικανή για τήρηση δεδομένων που ανήκουν στην Εταιρεία.

9. Τηλεργασία

Η συγκεκριμένη πολιτική τίθεται σε ισχύ κατόπιν έγκρισης της Διοίκησης. Ο/Η εργαζόμενος/η θα πρέπει προηγουμένως να λάβει τη σχετική έγκριση από το αρμόδιο τμήμα ή τον/την υπεύθυνό/η του/της. Η συγκεκριμένη πολιτική καθορίζει τα βασικά ζητήματα ασφάλειας πληροφοριών που πρέπει να εξετάζονται για κάθε συμφωνία μιας σύμβασης τηλεργασίας. Διασφαλίζει ότι όλα τα αναγκαία ζητήματα αντιμετωπίζονται και ότι τα πληροφοριακά αγαθά της Εταιρείας προστατεύονται.

Η παρούσα πολιτική δεν ασχολείται με τις πτυχές του ανθρώπινου δυναμικού της τηλεργασίας, όπως η υγεία, η ασφάλεια, η παρακολούθηση των απουσιών, η απόδοση στην εργασία και άλλα



παρόμοια συμβατικά θέματα. Τέτοια θέματα εμπίπτουν στις αρμοδιότητες του τμήματος Ανθρώπινου Δυναμικού και πρέπει να έχουν αποφασιστεί, πριν από την έναρξη της σύμβασης τηλεργασίας.

9.1 Εξοπλισμός

- Για τους σκοπούς της τηλεργασίας και για την απομακρυσμένη πρόσβαση στα επιχειρησιακά δίκτυα της Εταιρείας, μπορεί να χρησιμοποιηθεί μόνο ο εξοπλισμός που παρέχεται από την Εταιρεία. Ιδιωτικές συσκευές του εργαζομένου, όπως φορητοί υπολογιστές ή tablet/smartphones δεν πρέπει να χρησιμοποιούνται για το σκοπό αυτό, εκτός και αν υπάρχει σχετική έγκριση από τον Υπεύθυνο Πληροφορικής / CISO.
- Σύμφωνα με τις απαιτήσεις, στον τηλεργαζόμενο μπορεί να παρέχεται ένας φορητός ή σταθερός υπολογιστής με πληκτρολόγιο και ποντίκι. Ο εξοπλισμός παραμένει ιδιοκτησία της Εταιρείας ακόμη και μετά τη λήξη της συνεργασίας με τον υπάλληλο.
- Οι Διαχειριστές Συστημάτων της Εταιρείας είναι αρμόδιοι για την ρύθμιση του αναγκαίου εξοπλισμού, για κάθε ξεχωριστή περίπτωση τηλεργασίας.
- Όπου είναι εφικτό, η απομακρυσμένη θέση τηλεργασίας πρέπει να εποπτεύεται και να γίνεται εκτίμηση του κινδύνου της, πριν αποφασιστούν τα μέτρα ασφάλειας που πρέπει να χρησιμοποιηθούν.
- Κάθε τηλεργαζόμενος πρέπει να έχει ενημερωθεί για τους κινδύνους της τηλεργασίας και να έχει εκπαιδευτεί κατάλληλα στους τρόπους αντιμετώπισής τους.
- Ο τηλεργαζόμενος πρέπει να αποδέχεται πως αντιλαμβάνεται τους κινδύνους, τα δικαιώματα και τις υποχρεώσεις του ως προς τον ρόλο που του ανατίθεται και να υπογράφει σχετική υπεύθυνη δήλωση.
- Ο τηλεργαζόμενος είναι υπεύθυνος, ώστε να διασφαλίζει πως κανένας δεν έχει πρόσβαση στο τερματικό εργασίας του.
- Ο τηλεργαζόμενος είναι υπεύθυνος για τυχόν πληροφορίες της Εταιρείας, που μπορεί διαρρεύσουν, ως αποτέλεσμα δικής του αμέλειας (πχ. αν ξεχάσει έγγραφα στο χώρο τηλεργασίας).
- Ο εξοπλισμός τηλεργασίας πρέπει να ασφαρίζεται κατάλληλα, κάθε φορά που ο τηλεργαζόμενος διακόπτει την εργασία του (πχ. χρήση λουκέτων, ειδικών φοριαμών κλπ.).
- Μετά την εφαρμογή όλων των προαπαιτούμενων μέτρων ασφαλείας στην απομακρυσμένη τοποθεσία τηλεργασίας, η αυθεντικοποίηση του τηλεργαζόμενου ακολουθεί την ίδια διαδικασία που ακολουθούν και οι υπάλληλοι τοπικά στα γραφεία της Εταιρείας.





9.2 Επικοινωνίες

Εκτός από τον εξοπλισμό, ο τηλεργαζόμενος όταν αυτό καθίσταται δυνατό, πρέπει να χρησιμοποιεί ξεχωριστή σύνδεση διαδικτύου που δεν επικοινωνεί με τα υπάρχοντα οικιακά ευρυζωνικά δίκτυα. Αυτό γίνεται για να εξασφαλιστεί ότι:

- Η απόδοση του δικτύου δεν θα πρέπει να επηρεάζεται από άλλες δραστηριότητες στο σπίτι.
- Η δυνατότητα σύνδεσης άλλων συσκευών σε αυτή τη σύνδεση, μπορεί να προληφθεί μέσω της προστασίας των κλειδιών δικτύου κλπ.

Κάθε απομακρυσμένη σύνδεση τηλεργασίας πρέπει να τερματίζεται αμέσως μόλις διακόπτεται η εργασία του τηλεργαζόμενου.

9.3 Λήψη αντιγράφων ασφαλείας στην Τηλεργασία

- Όπου είναι δυνατόν, τα δεδομένα δεν πρέπει να αποθηκεύονται στον υπολογιστή του τηλεργαζόμενου. Σε περίπτωση που αυτό είναι αναπόφευκτο, είναι ευθύνη του τηλεργαζόμενου να διασφαλίσει ότι τα αντίγραφα ασφαλείας θα αποθηκεύονται για όσο το δυνατόν μικρότερο χρονικό διάστημα εκτός του εταιρικού δικτύου και θα μεταφέρονται το συντομότερο δυνατόν στο επιχειρησιακό δίκτυο της Εταιρείας.
- Δεν πρέπει να αποθηκεύετε τα μη κρυπτογραφημένα αντίγραφα ασφαλείας σε άλλες υπηρεσίες υπολογιστικού νέφους (cloud services) πλην αυτών που έχει ορίσει ο Διαχειριστής του Συστήματος.

9.4 Καταγγελία Σύμβασης

- Σε περίπτωση που η σύμβαση τηλεργασίας τερματιστεί για οποιονδήποτε λόγο, όλος ο εξοπλισμός που παρέχεται ως μέρος της σύμβασης πρέπει να επιστραφεί στον Υπεύθυνο Πληροφορικής / CISO και στη Διεύθυνση Πληροφορικής το συντομότερο δυνατόν.

10. Πολιτική Κρυπτογραφίας

Η Εταιρεία, όπου είναι τεχνικά εφικτό δύναται να εφαρμόζει πολιτική για τη χρήση κρυπτογραφικών μέτρων για την προστασία των κρίσιμων πληροφοριών της. Κρυπτογραφικές μέθοδοι χρησιμοποιούνται στους κωδικούς πρόσβασης για τη διαχείριση των κρίσιμων συστημάτων και των λογαριασμών της Εταιρείας όταν αυτοί αποθηκεύονται ή μεταφέρονται μέσω του δικτύου. Επιπλέον, φορητά αποθηκευτικά μέσα που περιέχουν πληροφορίες της Εταιρείας προστατεύονται με τους κατάλληλους κρυπτογραφικούς μηχανισμούς.

Η κρυπτογράφηση πρέπει να εφαρμόζεται για τα ευαίσθητα περιουσιακά στοιχεία πληροφοριών, τόσο κατά τη μεταφορά όσο και κατά την ηρεμία, με βάση την αξιολόγηση των κινδύνων και των νομικών/κανονιστικών απαιτήσεων.





Οι αλγόριθμοι κρυπτογράφησης και τα μήκη κλειδίων πρέπει να επιλέγονται με βάση τις βέλτιστες πρακτικές του κλάδου και τη συμμόρφωση με τα ισχύοντα πρότυπα.

Ισχυρή κρυπτογράφηση πρέπει να χρησιμοποιείται για ασύρματες επικοινωνίες, απομακρυσμένη πρόσβαση και κάθε άλλη ευαίσθητη μετάδοση δεδομένων.

Εφαρμόζεται κρυπτογράφηση σε όλες τις συσκευές ακόμα και στην τηλεργασία, με σκοπό την προστασία των διαβαθμισμένων πληροφοριών, εάν η συσκευή παρέχεται με κρυπτογράφηση, τότε δεν πρέπει να την απενεργοποιήσετε.

Όταν οι πληροφορίες πρόκειται να μεταφερθούν μέσω ενός δημόσιου δικτύου, όπως το Διαδίκτυο, τότε πρέπει να χρησιμοποιείται ισχυρή κρυπτογράφηση μέσω SSL, για τη διασφάλιση της εμπιστευτικότητας των δεδομένων που διαβιβάζονται. Συγκεκριμένα, πρέπει να εγκατασταθούν έμπιστα πιστοποιητικά στους δικτυακούς ιστότοπους της Εταιρείας με μέγεθος κλειδιού τουλάχιστον 2048 bits.

Επίσης, όλες οι συσκευές Bluetooth πρέπει να χρησιμοποιούν Secure Simple Pairing με ενεργοποιημένη την κρυπτογράφηση.

Πάροχοι Υπηρεσιών κρυπτογράφησης:

Κατά την πρόσληψη τρίτων παρόχων κρυπτογραφικών υπηρεσιών, ο οργανισμός πρέπει να διασφαλίζει ότι αυτοί τηρούν τις βέλτιστες πρακτικές του κλάδου, διαθέτουν σχετικές πιστοποιήσεις και συμμορφώνονται με τις νομικές και κανονιστικές απαιτήσεις.

Οι συμβάσεις ή οι συμφωνίες με τους παρόχους κρυπτογραφικών υπηρεσιών πρέπει να καθορίζουν σαφώς τους ρόλους, τις αρμοδιότητες και τις απαιτήσεις ασφαλείας.

11. Φυσική και Περιβαλλοντική Ασφάλεια

Όλα τα μέλη του προσωπικού πρέπει να εφαρμόζουν τις πολιτικές και τις διαδικασίες ασφαλείας της Εταιρείας που αφορούν στη φυσική και περιβαλλοντική προστασία των πληροφοριακών της αγαθών, έτσι ώστε να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση, καθώς και η καταστροφή και η επέμβαση στις εγκαταστάσεις και τις πληροφορίες του.

11.1 Ασφαλείς Περιοχές

Η Εταιρεία εφαρμόζει όλα τα απαραίτητα μέτρα προκειμένου να διασφαλίσει ότι οι περιοχές που περιέχουν πληροφορίες και συστήματα επεξεργασίας πληροφοριών προστατεύονται επαρκώς.

Παράλληλα λαμβάνονται κατάλληλα μέτρα έτσι ώστε να εξασφαλίζεται η φυσική προστασία της Εταιρείας αναφορικά με όλες τις μορφές φυσικής ή προκαλούμενης από τον άνθρωπο καταστροφής (π.χ. φωτιές, πλημμύρες, εκρήξεις κ.λπ.).





11.2 Ασφάλεια Εξοπλισμού

Οι Διευθύνσεις / Τμήματα της Εταιρείας καθίστανται υπεύθυνοι για την εφαρμογή μέτρων που αφορούν στη φυσική ασφάλεια των προσωπικών υπολογιστών και των πληροφοριακών αγαθών στο χώρο ευθύνης τους, συμπεριλαμβανομένων μέτρων για την αποφυγή περιστατικών κλοπής, βανδαλισμού ή καταστροφής εξοπλισμού και αποθηκευτικών μέσων.

12. Ασφάλεια Επιχειρησιακών Λειτουργιών

12.1 Λειτουργικές Διαδικασίες

Όλες οι αρμοδιότητες και διαδικασίες για τη διαχείριση και τη λειτουργία όλων των εγκαταστάσεων επεξεργασίας πληροφοριών, συμπεριλαμβανομένων των διαδικασιών απόκρισης και αντιμετώπισης περιστατικών ασφάλειας, καταγράφονται. Πρόσβαση σε κρίσιμα πληροφοριακά συστήματα και δεδομένα παρέχεται μόνο εφόσον πιστοποιείται η αντίστοιχη ανάγκη. Εφαρμόζεται καταμερισμός αρμοδιοτήτων, όπου είναι εφικτό, προς αποφυγή ή ελαχιστοποίηση των κινδύνων από σκόπιμη κακή χρήση των συστημάτων ή από αμέλεια.

Για την προστασία των λειτουργικών διαδικασιών της Εταιρείας πρέπει να εφαρμόζονται τα παρακάτω:

Προστασία από Κακόβουλο Λογισμικό: Λογισμικό ανίχνευσης ιών χρησιμοποιείται σε όλους τους σταθμούς εργασίας, εξυπηρετητές και φορητούς υπολογιστές σύμφωνα με την «Πολιτική Ασφάλειας Λειτουργιών».

Αντίγραφα Ασφάλειας: Αντίγραφα ασφάλειας Πληροφοριών και λογισμικού λαμβάνονται σε τακτά χρονικά διαστήματα σύμφωνα με την «Πολιτική Αντιγράφων Ασφαλείας».

Έλεγχος: Ακολουθούνται διαδικασίες για την παρακολούθηση της χρήσης των συστημάτων της Εταιρείας, ενώ στο μέτρο που είναι δυνατό και τεχνικά εφικτό, οι δραστηριότητες όλων των χρηστών της Εταιρείας θα καταγράφονται και θα ελέγχονται σε τακτά χρονικά διαστήματα. Τα συστήματα καταγραφής και οι καταγεγραμμένες πληροφορίες θα προστατεύονται επαρκώς από τους κινδύνους της μη εξουσιοδοτημένης πρόσβασης και τροποποίησης ή καταστροφής τους.

Έλεγχος Νέου Λογισμικού: Για την ανάπτυξη και την εγκατάσταση νέων εφαρμογών, ο Υπεύθυνος Έργου θα τεκμηριώνει τις απαιτήσεις ασφάλειας της Εταιρείας και θα τις ανασκοπεί ο Υπεύθυνος Πληροφορικής ή CISO, κατά τη διάρκεια της φάσης ανάλυσης απαιτήσεων του έργου.

Διαχείριση Τεχνικών Ευπαθειών: Ο Υπεύθυνος Πληροφορικής της Εταιρείας πρέπει να εφαρμόζει τις ενημερώσεις ή διορθώσεις ασφάλειας έγκαιρα και σύμφωνα με όσα αναφέρονται στη «Πολιτική Ασφάλειας Λειτουργιών».



Έλεγχος των Πληροφοριακών Συστημάτων: Οι απαιτήσεις και διαδικασίες ελέγχου των πληροφοριακών συστημάτων πρέπει να σχεδιάζονται προσεκτικά με σκοπό να ελαχιστοποιηθεί ο κίνδυνος διατάραξης της ομαλής λειτουργίας των πληροφοριακών συστημάτων της Εταιρείας.

13. Ασφάλεια Δικτύων και Επικοινωνιών

Τα δίκτυα της Εταιρείας διαχειρίζονται και ελέγχονται, προκειμένου να εξασφαλίζεται η επαρκής προστασία από απειλές και η διατήρηση της ασφάλειας των συστημάτων, των εφαρμογών και των πληροφοριών που χρησιμοποιούν.

Η Μηχανογράφηση της Εταιρείας διασφαλίζει την αξιοπιστία και τη λειτουργικότητα της δικτυακής υποδομής, τη δυνατότητα εύκολης πρόσβασης των χρηστών στους πληροφοριακούς πόρους και την προστασία της εμπιστευτικότητας και της ακεραιότητας των πληροφοριών της Εταιρείας.

Όλες οι συνδέσεις δικτύων της Εταιρείας, είτε μισθωμένες από τρίτους, είτε ιδιόκτητες, είτε δημόσιες προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, Η Εταιρεία λαμβάνει τα κατάλληλα μέτρα για την προστασία της μετάδοσης των πληροφοριών και των μηνυμάτων της όπως ορίζεται στην «Πολιτική Ασφάλειας Δικτύων και Επικοινωνιών».

14. Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων

Για την ανάπτυξη και συντήρηση των Πληροφοριακών Συστημάτων της Εταιρείας λαμβάνονται υπόψη τα παρακάτω:

Απαιτήσεις Ασφάλειας Πληροφοριακών Συστημάτων: Πριν από την ανάπτυξη νέων πληροφοριακών συστημάτων ή την προσθήκη νέων λειτουργιών στα υπάρχοντα, πραγματοποιείται **εκτίμηση κινδύνου** ώστε οι απαιτήσεις ασφάλειας να συμπεριλαμβάνονται στο σχεδιασμό των νέων πληροφοριακών συστημάτων.

Η ανάπτυξη των νέων πληροφοριακών συστημάτων πραγματοποιείται σε ασφαλές / δοκιμαστικό περιβάλλον που δεν επηρεάζει τα παραγωγικά συστήματα. Η συγκεκριμένη διαδικασία εφαρμόζεται σε όλο τον κύκλο ζωής ενός συστήματος.

Στις κρίσιμες εφαρμογές της Εταιρείας ενσωματώνονται έλεγχοι επικύρωσης όπου υποστηρίζεται και είναι τεχνικά εφικτό, έτσι ώστε να είναι δυνατό να ανιχνεύονται οποιεσδήποτε ενέργειες τροποποίησης ή καταστροφής πληροφοριών που μπορεί να προκληθούν από λάθη ή σκόπιμες ενέργειες.

Ασφάλεια στις Διαδικασίες Ανάπτυξης και Υποστήριξης: Η Εταιρεία εφαρμόζει μια επίσημη διαδικασία ελέγχου αλλαγών και δοκιμαστικών ελέγχων όπως ορίζεται στη «Πολιτική Ανάπτυξης και Συντήρησης Πληροφοριακών Συστημάτων». Έτσι διασφαλίζεται ότι δεν υπάρχουν επιπτώσεις στις λειτουργίες ή την ασφάλεια των συστημάτων της Εταιρείας από αλλαγές σε νέα / υπό υλοποίηση κρίσιμα πληροφοριακά συστήματα.



Διαχείριση Τεχνικών Ευπαθειών: Η Εταιρεία στο πλαίσιο ενημέρωσης από τους προμηθευτές σχετικά με τις τεχνικές ευπάθειες των πληροφοριακών του συστημάτων λαμβάνει πληροφορίες, έτσι ώστε να προβαίνει άμεσα στην αντιμετώπιση των σχετικών κινδύνων.

15. Διαχείριση Περιστατικών Ασφάλειας

Η Εταιρεία εφαρμόζει αναλυτική διαδικασία (βλέπε «ΔΙ-5 Διαδικασία Διαχείρισης Περιστατικών») κατά την οποία τα περιστατικά ασφάλειας καταγράφονται, κατηγοριοποιούνται με κριτήριο τις πιθανές επιπτώσεις στη λειτουργία της Εταιρείας και θα αποφασίζεται ο κατάλληλος τρόπος αντιμετώπισής τους.

Αναφορά Περιστατικών Ασφάλειας: Όλοι οι υπάλληλοι, οι ανάδοχοι και τα τρίτα μέρη που χρησιμοποιούν τα πληροφοριακά συστήματα και τις υπηρεσίες της Εταιρείας, πρέπει να αναφέρουν άμεσα στο Τμήμα Πληροφορικής, περιστατικά που αφορούν στην ασφάλεια των πληροφοριών της Εταιρείας.

Διαχείριση Περιστατικών Ασφάλειας και Βελτιώσεων: Η Εταιρεία στο πλαίσιο της διαχείρισης περιστατικών ασφάλειας εφαρμόζει κατάλληλες πολιτικές και διαδικασίες, έτσι ώστε να εξασφαλίζεται η έγκαιρη, μεθοδική και αποτελεσματική αντιμετώπιση των περιστατικών ασφαλείας.

16. Διαχείριση Επιχειρησιακής Συνέχειας

Στο πλαίσιο της πολιτικής ασφάλειας της Εταιρείας τηρείται και εφαρμόζεται πολιτική και αναλυτικές διαδικασίες αναφορικά με τη δημιουργία, την εφαρμογή, την ενημέρωση και την παρακολούθηση του «Σχεδίου Επιχειρησιακής Συνέχειας», ώστε να εξασφαλίζεται η ελάχιστη δυνατή διακοπή στις λειτουργίες της Εταιρείας σε περιπτώσεις φυσικών καταστροφών ή διακοπής της λειτουργίας σημαντικών πληροφοριακών του πόρων.

Ο Υπεύθυνος IT και οι ιδιοκτήτες πληροφοριών θα εξετάζουν σε τακτά χρονικά διαστήματα την ετοιμότητα της Εταιρείας να εφαρμόσει το Σχέδιο Επιχειρησιακής Συνέχειας. Το Σχέδιο αυτό πρέπει να εξασφαλίζει ότι οι πληροφορίες θα είναι διαθέσιμες όποτε αυτές ζητηθούν από εξουσιοδοτημένους χρήστες. Τα συστήματα αντιγράφων ασφαλείας ελέγχονται σε προκαθορισμένα διαστήματα, ούτως ώστε να ελαχιστοποιείται ο κίνδυνος αδυναμίας ανάκτησης κρίσιμων δεδομένων.

17. Λίστα Πολιτικών, Διαδικασιών & Φορμών

Η Εταιρεία έχει τεκμηριώσει και διατηρεί όλες τις απαιτούμενες, από το πρότυπο ISO 27001 πολιτικές, διαδικασίες και φόρμες του ΙΣΜΣ.





Η λίστα με τις πολιτικές και διαδικασίες ασφάλειας αποτυπώνονται στους παρακάτω πίνακες.

17.1 Πίνακας Πολιτικών

Κωδικός	Όνομα Πολιτικής
ΜΑ-00	Εγχειρίδιο Ασφάλειας Πληροφοριών
ΠΟ-00	Πολιτική Ασφάλειας Πληροφοριών
ΠΟ-01	Πολιτική Αποδεκτής Διαχείρισης Αγαθών
ΠΟ-02	Πολιτική Διαχείρισης Αλλαγών
ΠΟ-03	Πολιτική Διαβάθμισης Πληροφοριών
ΠΟ-04	Πολιτική Διαχείρισης Επιχειρησιακής Συνέχειας
ΠΟ-05	Πολιτική Διαχείρισης Προμηθευτών
ΠΟ-06	Πολιτική Ελέγχου Πρόσβασης
ΠΟ-07	Πολιτική Διαχείρισης Ενημερώσεων Υλικού και Λογισμικού
ΠΟ-08	Πολιτική Ασφάλειας Λειτουργιών
ΠΟ-09	Πολιτική Οργάνωσης Ασφάλειας Πληροφοριών
ΠΟ-10	Πολιτική Αντιγράφων Ασφαλείας
ΠΟ-11	Πολιτική Ασφάλειας Δικτύων και Επικοινωνιών
ΠΟ-12	Πολιτική Διαχείρισης Κινδύνων ΤΠΕ
ΠΟ-13	Πολιτική Συμμόρφωσης
ΠΟ-14	Πολιτική Αναφοράς προς Εποπτικές Αρχές
ΠΟ-15	Πολιτική Ανάπτυξης και Συντήρησης Πληροφοριακών Συστημάτων
ΠΟ-16	Πολιτική Υπηρεσιών Υπολογιστικού Νέφους
ΠΟ-17	Πολιτική Αποδέσμευσης από Παρόχους Υπηρεσιών ΤΠΕ
ΠΟ-18	Πολιτική Διαχείρισης Περιστατικών Ασφαλείας
ΠΟ-19	Πολιτική Κρυπτογράφησης και Χειρισμού Ευαίσθητων Δεδομένων
ΠΟ-20	Πολιτική Δοκιμών Ψηφιακής Ανθεκτικότητας



ΠΟ-21	Πολιτική Εκπαίδευσης και Ευαισθητοποίησης Χρηστών
ΠΟ-22	Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας

17.2 Πίνακας Διαδικασιών

Κωδικός Πολιτικής	Όνομα
ΔΙ-1	ΔΙ-1 Έκθεση Εσωτερικού Ελέγχου
ΔΙ-1-2	ΔΙ-1-2 Πλάνο Εσωτερικών Ελέγχων
ΔΙ-1-3	ΔΙ-1-3 Διαδικασία Εσωτερικού Ελέγχου
ΔΙ-2	ΔΙ-2 Διαδικασία Διορθωτικών Ενεργειών
ΔΙ-3	ΔΙ-3 Διαδικασία Ελέγχου Εγγράφων
ΔΙ-3-1	ΔΙ-3-1 Αρχείο Ελεγχόμενων Εγγράφων ΣΔΑΠ
ΔΙ-4	ΔΙ-4 Διαδικασία Ελέγχου Αρχείων
ΔΙ-5	ΔΙ-5 Διαδικασία Διαχείρισης Περιστατικών
ΔΙ-6	ΔΙ-6 Διαδικασία Ανασκόπησης Διοίκησης
ΔΙ-7	ΔΙ-7 Διαδικασία Διαχείρισης Αλλαγών
ΔΙ-8	ΔΙ-8 Διαδικασία Πρόσβασης Χρηστών
ΔΙ-8-1	ΔΙ-8-1 Διαδικασία Αξιολόγησης Φορητών Ιδιωτικών Συσκευών
ΔΙ-8-2	ΔΙ-8-2 Διαδικασία Καταχώρισης Πληροφοριακών Αγαθών
ΔΙ-9	ΔΙ-9 Πειθαρχική Διαδικασία
ΔΙ-10	ΔΙ-10 Διαδικασία Καταστροφής Μέσων Αποθήκευσης
ΔΙ-11	ΔΙ-11 Διαδικασία Εκτίμησης Κινδύνου
ΔΙ-12	ΔΙ-12 Διαδικασία Ασφαλούς Ανάπτυξης Συστημάτων
ΔΙ-13	ΔΙ-13 Διαδικασία Λήψης Αντιγράφων Ασφάλειας
ΔΙ-14	ΔΙ-14 Αρχείο Δραστηριοτήτων Επεξεργασίας
ΔΙ-15	ΔΙ-15 Διαδικασία Λειτουργίας Διαχείρισης
ΔΙ-16	ΔΙ-16 Διαδικασία Μεταφοράς Εξοπλισμού



ΔΙ-17	ΔΙ-17 Εκπαίδευση Υπευθύνου ΣΔΑΠ, Ομάδας Ασφάλειας & Εμπλεκόμενων
ΔΙ-18	ΔΙ-18 Διαδικασία Δοκιμών Ψηφιακής Ανθεκτικότητας
ΔΙ-19	ΔΙ-19 Σχέδιο Επιχειρησιακής Συνέχειας και Αποκατάσταση
ΔΙ-20	ΔΙ-20 Διαδικασία Φυσικής Πρόσβασης
ΔΙ-21	ΔΙ-21 Διαχείρισης Αφαιρούμενων Μέσων
ΔΙ-21-1	ΔΙ-21-1 Αίτησης Χρήσης Αφαιρούμενου
ΔΙ-22	ΔΙ-22 Πληροφόρηση απειλών
ΔΙ-23	ΔΙ-23 Επιτήρηση Φυσικής Ασφάλειας
ΔΙ-24	ΔΙ-24 Διαχείριση Ασφαλών Παραμετροποιήσεων
ΔΙ-25	ΔΙ-25 Διαγραφή Πληροφοριών
ΔΙ-26	ΔΙ-26 Διαδικασία Κρυπτογράφησης και Χειρισμού Ευαίσθητων Δεδομένων
ΔΙ-27	ΔΙ-27 Αποτροπή Διαρροής Πληροφοριών
ΔΙ-28	ΔΙ-28 Επίβλεψη Δραστηριοτήτων
ΔΙ-29	ΔΙ-29 Προστασία Διαδικτυακής Πρόσβασης
ΔΙ-30	ΔΙ-30 Διαδικασία Ασφάλεια Υπολογιστικού Νέφους
ΔΙ-31	ΔΙ-31 Συνεχής Βελτίωση & Στόχοι
ΔΙ-31-1	ΔΙ-31-1 Εσωτερική Επιθεώρηση
ΔΙ-32	ΔΙ-32 Διαδικασία Διαχείρισης Τρίτων Μερών





17.3 Πίνακας φορμών

Κωδικός Πολιτικής	Όνομα
ΦΟ-1	ΦΟ-1 Λίστα Ελέγχου Εσωτερικού Ελέγχου
ΦΟ-2	ΦΟ-2 Φόρμα Διορθωτικών Ενεργειών
ΦΟ-3	ΦΟ-3 Φόρμα Αίτησης Αλλαγών Εγγράφου
ΦΟ-5-1	ΦΟ-5-1 Φόρμα Αναφοράς Περιστατικού Αδυναμίας Ασφάλειας
ΦΟ-5-2	ΦΟ-5-2 Αρχείο Περιστατικών
ΦΟ-5-3	ΦΟ-5-3 Φόρμα Καταγραφής Περιστατικών
ΦΟ-6	ΦΟ-6 Φόρμα Πρακτικών Ανασκόπησης ΔΣ
ΦΟ-7	ΦΟ-7 Φόρμα Αίτησης Αλλαγών
ΦΟ-8	ΦΟ-8 Έντυπο Καταχώρισης Πληροφοριακού. Αγαθού
ΦΟ-8-1	ΦΟ-8-1 Έντυπο Καταχώρισης Πληροφοριακού. Αγαθού
ΦΟ-8-2	ΦΟ-8-2 Φόρμα Δικαιωμάτων Πρόσβασης
ΦΟ-8-3	ΦΟ-8-3 Φόρμα Χρέωσης Αγαθών
ΦΟ-8-4	ΦΟ-8-4 Φόρμα Χρέωσης Αγαθών Εκτός Εταιρείας
ΦΟ-8-5	ΦΟ-8-5 Μητρώο Χρέωσης Αγαθών Εκτός Εταιρείας
ΦΟ-8-6	ΦΟ-8-6 Φόρμα Αίτησης Υπηρεσίας
ΦΟ-8-7	ΦΟ-8-7 Μητρώο αιτήσεων υπηρεσιών
ΦΟ-8-9	ΦΟ-8-9 Φόρμα Δικαιωμάτων Πρόσβασης
ΦΟ-8-10	ΦΟ-8-10 Μητρώο Χρηστών Απομακρυσμένης Πρόσβασης
ΦΟ-13-1	ΦΟ-13-1 Φόρμα Αξιολόγησης Δοκιμών Ανάκτησης
ΦΟ-13-2	ΦΟ-13-2 Φόρμα Αρχείων Καταγραφής Επαναφοράς
ΦΟ-20	ΦΟ-20 Βιβλίο Καταγραφής Επισκεπτών
ΦΟ-20-1	ΦΟ-20-1 Έντυπο Παραλαβής-Παράδοσης
ΦΟ-20-2	ΦΟ-20-2 Έντυπο Αλυσίδας Φύλαξης



ΦΟ-21	ΦΟ-21 Αρχείο Αιτήσεων Χρήσης
ΦΟ-31	ΦΟ-32 Στόχοι Ασφάλειας
ΦΟ-31-1	ΦΟ-32-1 Καταγραφή ΜΣ
ΦΟ-31-2	ΦΟ-32-2 Πρακτικά Συμβουλίου

17.4 Πίνακας μητρώων και λοιπών εγγράφων

Κωδικός Πολιτικής	Όνομα
EK-00	Risk Assessment Report_Rener_Alphabit_2025
EK-01	RENER 2025-ALPHABIT-Risk-Assessment
ΣΧ-00	ΣΧ-00_Σχέδιο_Αντιμετώπισης_Κινδύνου
MH-7	MH-7 Μητρώο Αιτημάτων Αλλαγών
MH-10	MH-10 Μητρώο Διαγραφής Καταστροφής Αγαθών
MH-11-20	MH-11-20 Μητρώο Εξουσιοδοτημένων Χρηστών
MH-13	MH-13 Μητρώο Προγράμματος Αντιγράφων Ασφαλείας
MH-18	MH-18 Μητρώο Ευπαθειών
MH-18-1	MH-18-1 Μητρώο Κινδύνων
MH-31	MH-31 Μητρώο Δικτύου
ΣΧ-6	ΣΧ-6 Σχέδιο Δράσης
ΠΡ-1	ΠΡ-1 Πρακτικό Ανασκόπησης Διοίκησης
EK-17-1	Training - Security Management ISO 27001
EK-17-2	Training - Security Policies ISO27001
MH-32	MH-32 Μητρώο_Δικτύου
EK-33	Μελέτη Εκτίμησης Κινδύνου Τρίτων Μερών
MH-33	Μητρώο Τρίτων Παρόχων - RENER ENERGY S.A